特定非営利活動法人
日本システム監査人協会報

2011 年 12 月発行
No 130

No.130（2011 年 12 月　発行）

会報電子版の記事　目次

めだか　【 １年の評価と見直しは年（度）末でいいのか 】　　投稿

12月になるとまた思い出してしまいます。新年を迎える年末、大晦日が近づいていること。
1年の計は元旦にあり、などと勇んで計画を立てたものの、その結果はどうでしょうか。
まだひと月あると言わずに、ここは計画当初からの活動結果を振り返ってみましょう。

まず、どのような計画を作ったのか覚えているでしょうか。覚えていない計画は論外でしょう。
アイデアや思いつきと計画では明らかに内容が違います。（この部分はよく勘違いするのですが）
覚えきれないほどの計画、単にアイデアや夢があるだけで、具体的な計画ではないでしょうか。

計画というからには、達成目標があって、その目標は実現可能で、またその計画は実践方法が具体化されていなければなりません。この計画、実践、評価、見直しの流れをつないでPDCAとして管理する手法は、あまりにも身近すぎて、ついおろそかにしてしまいがちなので要注意です。

システム化計画、システム化開発、システム化運用・保守、プロジェクトマネジメントなどの分野に、あるいはシステム監査の分野にも計画を作成するための手続があります。それらの計画は、企業などの組織内で実行するための計画です。誰がどのように役割分担して実行するのか、計画を起案して評価承認し、予算や手段に無理やムダがないか、技術面や複雑な環境面から困難が予想される分野を異なる立場で評価して、確実に目標達成するための仕組みが考えられています。しかしながら実践面では、当初想定外の出来事が起きます。そこでリスクアセスメント、リスクマネジメント、さらに事業継続（BCP/BCM）という考えが登場します。

リスクマネジメント、BCMの考えかたでは、リスクや障害の内容を事前に分析しておき、発生する場合にどのように対処するのか、その対処方法を予め計画しておき、リスクが現実に発生した場合に慌てず清々と対処できるようにするためのものですね。このようにリスクマネジメント、BCMの分野でもPDCAが活用されます。

1年の活動評価と見直しは、年末にある。企業や組織での仕事の場合には、年度末にある。
だからといって、年末や年度末まで待つ必要はなく、この見直しは早いほうがいいでしょう。
つまり、毎日のように評価することで、改善点を把握し、実施改善手段の変更をこまめに実現すると、目標達成がよりスムーズに、そして早く実現できることは、いろいろな経験でわかってきます。
ITを活用した評価の手法は、より具体的に計画値を設定して測定し、計画と実際の違いを細かに比較することで、不足すること、計画修正の必要性を、即時に、また設定したタイミングで知ることができます。
自己評価の分野は、自動化ツールの開発、実装とともに、どんどん拡大しています。

さて今年の2011年もいろいろなことが起こりましたが、流行語大賞など、今年の世相を反映した用語が選ばれて報告されるでしょう。システム監査の分野ではどうでしょうか。　　（自省）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

めだか　【歴史にみる監査　－　ガバナンスについて歴史をふりかえって 】　　投稿

中国の「唐」帝国は繁栄をきわめ、日本からも平安時代に遣唐使が派遣され先進的な制度や文化をとりいれています。陳舜臣著「小説十八史略5Ⅲ太子たちの悲劇」から引用してその制度を顧みてみます。

唐の政治の中心は三省六部であった。

中書省（長官は中書令）で詔勅の草案をつくり、門下省（長官は侍中）にまわす。そこで検討し、意見を加えて、中書省へ差し戻すのである。こうして詔勅ができあがり、それを執行するのが尚書省（長官は尚書令）であった。尚書令の下に行政機関として六部がある。吏部（内政）、戸部（財政）、礼部（文教）、兵部（軍事）、刑部（法務）、工部（建設）の六部なのだ。

三省の長官が通称「宰相」である。ただし、尚書令は唐一代、空位とされた。太宗が太子時代に就任した官なので、臣下が同じ職につくのを遠慮したのだ。そして、六部を二つに分け、左僕射と右僕射が三部ずつを統轄することになり、この左右の僕射が宰相の一員とみなされたのである。

（中略）

門下省は詔勅の草案に意見を述べるので、その長官の侍中は、時代によって、「納言（のうげん）」と呼ばれたこともある。唐制を採りいれた日本では、これに相当する職を「大納言（だいなごん）」と呼んだ。

「唐」帝国のガバナンスは以上のような唐制に支えられて「唐」の繁栄はつづいたわけです。日本の律令制では、左大臣、右大臣と、大納言、中納言などがあって、それらはどういうものか疑問を持っていました。日本では、大臣につぐ次官として処遇されていて、ガバナンスの主旨はなくなって、平安貴族は家柄で処遇が決まっていたようです。時代がくだっても、徳川将軍は太政大臣、尾張は大納言、前田は中納言というようになっています。

今回、この本の説明する唐制からその由来を知って疑問が解消しました。やはり、「納言」は、本来、組織体の維持のために執行権限をけん制するガバナンスの役職であったと思います。

日本の組織体ではガバナンスのための方法として「内部統制」が行われています。内部統制の中に「監査」があって、その中にITに関わる「システム監査」があります。あらためて、「システム監査」の役割は、情報システムの企画・開発・運用・保守等の局面において、執行権限を持つ者をけん制し、執行状況を検討し、意見を加えて、差し戻す役目であると思います。システム監査は、情報システムの執行状況のけん制ということから、企画の局面においても法令順守や情報セキュリティ等が妥当かどうかなどの観点から情報システムの企画に対するけん制は重要です。

組織体経営においてITへの依存度が高まっている現在、システム監査の重要性を会報やネットワークを通じて広報し続けていくことが必要であると思います。

（空心菜）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。 ）

研究会、セミナー開催報告、支部報告

■ 【第 166 回月例研究会講演録】

会員 No.2063　舩橋 真

■講演テーマ：金融業界の情報セキュリティについて

講師：公益財団法人　金融情報システムセンター　監査安全部　総括主任研究員　松宮　伸行　氏

講演日時：2011 年 9 月 28 日　午後 6 時半から

場所：お茶の水　総評会館

参加者：128 名

■講演の概要

講師は、三井住友銀行より公益財団法人　金融情報システムセンター（以下 FISC）に出向され、監査安全部にて安全対策およびシステム監査の普及・推進に携わっている。

今回、金融業界におけるセキュリティポリシーの重要性・策定手順、近年の金融機関を取り巻くセキュリティ脅威の動向について、FISC 策定の安全対策基準書との関係を交えて講演いただいた。

目次　1. セキュリティポリシーの策定の重要性
2. 安全対策基準書の概要
3. 金融機関を取り巻くセキュリティ脅威の動向
4. 最近の事故事例の紹介と分析
5. 報告者所感

報告

1. セキュリティポリシーの策定の重要性

（1）セキュリティポリシーとは「会社の情報資産を適切に保護するための会社としての安全対策に関する統一方針」であり以下の“3つの W”を記述することが肝要である。

・情報資産の保護の責任の所在の明記（WHO）
・何が重要でかつ守るべき情報資産なのか（WHAT）
・なぜ守るのか（WHY）

（2）セキュリティポリシー策定による効果

・社員がリスクに気がつき、どのように行動するべきかがわかるようになる。
・講じるべき安全対策の対象とレベル（何に対して、どの程度まで）が明確になる
・責任の所在が明確になる。

（3）保護の対象

・情報資産＝「情報」＋「情報システム」
・業務プロセスにおいて生じる、あらゆる情報を対象とする。マニュアルや企画書など物理的に存在するものから、経営会議の場で交わされる会話なども対象である。

(4)FISC の考えるドキュメントの体系

・セキュリティポリシー(基本方針)　⇒憲法にあたるもの。会社の基本方針

・セキュリティスタンダード　⇒個々の会社の安全対策基準

・マニュアル、手順書　⇒具体的で強制的な手順や操作方法を記述したもの

(5)セキュリティポリシーに関する社内の体制

①策定体制

情報保護レベルを高くすることにより業務効率が低下する可能性があることから、セキュリティポリシーを策定する場合は経営層の指示のもと、全社を巻き込んで策定する体制とすべき。

②運用体制

・セキュリティ管理部門　⇒全社のセキュリティを統括管理する専担組織。

・社内の各部門　⇒各部門の安全対策の実施と啓蒙、運用に関して責任を持つ。

・監査部門　⇒運用状況の監視、見直しの指示を行う部門

(6)セキュリティポリシー策定の順序

STEP1として、策定の意思決定フェーズ。経営層からセキュリティポリシー策定の承認を受け、この決定を受けた策定員会(タスクフォース)の発足。

STEP2としてセキュリティポリシー策定にむけた準備作業。以下の3つに分類。

・目的、目標の設定と明確化　⇒前述の3つのW(WHO 、WHAT、WHY)の明確化

・情報資産の洗出し　⇒会社として守るべき重要な情報の明確化

・脅威の認識とリスクの評価　⇒洗出した情報資産を取り巻く脅威の認識および、それらの脅威毎のリスクレベルの明確化

STEP3として目標とする対策についての原案の作成。

※現状の安全対策レベルではなく、より高い目標レベルで作成することが求められる。

※目標レベルが達成困難な場合の対応を経営層と認識を合わせ承認を得ておく必要がある。

STEP4として実際に業務で使用するマニュアル類の作成。(今回の講演では省略)

STEP5として策定したセキュリティポリシーに基づく安全対策の実施。策定したセキュリティポリシーに基づいた安全対策の中長期計画の立案(PLAN)、安全対策の実施(DO)、安全対策の評価(SEE)このサイクルを繰り返していく。

セキュリティポリシーとは経営者が発信するものでありむやみに変更されることは好ましくないことを留意する必要があるとのこと。ただし、セキュリティスタンダードについては、情報技術の進歩などに合わせた見直しや定期的な見直しが必要であり、見直しにあたっては監査部門の果たす役割が重要との認識であった。

2. 安全対策基準書の概要

FISC が策定した「安全対策基準」とは、情報システムが業務に必要不可欠な現状において、金融機関に対する社会的要請、障害時の影響の広域化・深刻化など、システム化に内在するスクについて、“どのような対策を、どこまでやるべきか？”との問いに対して金融機関等にとっての共通的な拠り所・指針となるべく策定された。

(1)策定目的および対象

自然災害、機器の障害、不正使用行為等から生ずる金融機関等コンピュータシステムの障害に対して以下の3点を目的としている。

・障害発生を未然に防止すること
・障害発生時の影響を最小化すること
・障害から早期の回復を図ること

また、対象となるのは金融機関のシステムのうち以下の物が対象である。
・顧客にオンラインサービスを提供するコンピュータシステム
・他の金融機関等との決済業務に使用するコンピュータシステム
・顧客データを扱うコンピュータシステム
・サービスを提供するために金融機関等が顧客に提供するハード、ソフト
※上記システム以外でもリスクを評価したうえで本基準を適用することが望まれる。

(2)安全対策基準書の構成
①前節
Ⅰ. 安全対策基準の考え方　Ⅱ. 安全対策基準書の利用に当たって　Ⅲ. 安全対策基準一覧表
②本編
Ⅳ. 設備基準　Ⅴ. 運用基準　Ⅵ. 技術基準
③後節(資料編)

(3)基準書の使い方
本編の各基準については以下の点に注意して使用する必要がある。
Ⅳ. 設備基準　⇒全体のシステム構成について設けた基準であり、「コンピュータセンター」や「本部・営業店」などによって適用する基準が異なる。
Ⅴ. 運用基準　⇒個々の会社の組織の実状や規模に応じて実効性のあるものとすること。
Ⅵ. 技術基準　⇒当基準書の技術基準は機能面から設けた基準となっているのでそれを理解したうえで適用する必要がある。

(4)FISC による金融機関に対しての安全対策実施状況のアンケート結果
2009年度分の集計結果では、明文化されたルールが無いものは 4.1%。前年度の 6.9%から比べると安全対策のルール化が進んでいる。なお、漏洩防止対策採用されているのは外部媒体の利用制限が最も多い。

3. 金融機関を取り巻くセキュリティ脅威の動向

(1)単純かつ極端に大規模なものと巧妙なものの二極化(マカフィー社資料にて)
2005 年くらいから見られた“金銭・情報目的の犯罪”について、より組織化・分業化によってより巧妙に進化する傾向である。また、2009 年頃からハクティビズム(ハッカー＋アクティビズム(≒積極行動主義)の造語)による“不特定多数による組織に対する抗議・反抗の行動”が出現している。

(2)不特定多数による、特定企業・個人を対象とした攻撃
フィッシングなど他に複数の方法を組み合わせた「新しいタイプの攻撃」(Advanced Persistent Threats＝高度に強靭な脅威)も見られるようになった。

(3)サイバー犯罪の一般化・役割分担

簡単に不正アクセスを可能とするツールが公開されていることから、詳しい知識の無い人間でもサイバー犯罪を起こせるようになった。また、情報窃取者と情報利用者の闇市場を介した役割分担も進んでいる。

(4)ウィルスなど開発の短期間化

ソフトの脆弱性対策の公開前に攻撃をする“ゼロデイ攻撃”が代表的なものである。

(5)2011 年版の 10 大脅威(独立行政法人　情報処理推進機構(IPA)作成)

1 位 「人」が起こしてしまう情報漏えい
2 位 止まらない！ウェブサイトを経由した攻撃
3 位 定番ソフトウェアの脆弱性を狙った攻撃
4 位 狙われだしたスマートフォン
5 位 複数の攻撃を組み合わせた新しいタイプの攻撃
6 位 セキュリティ対策備がもたらすトラブル
7 位 携帯電話向けウェブサイトのセキュリティ
8 位 攻撃に気づけない標的型攻撃
9 位 クラウド・コンピューティングのセキュリティ
10 位 ミニブログサービスや SNS の利用者を狙った攻撃

※4 位～7 位と 10 位については 2011 年に初めて登場。

1 位の“「人」が起こしてしまう情報漏えい”はいつも上位に入る脅威。システムで制御できない部分であり、最終的な判断を人が行っていることから生じるもの。

4 位 の“狙われだしたスマートフォン”は、Android OS やタブレット端末の普及に伴って増えてきており、FISC としてもセキュリティフォーラムに参加するなど研究を進めている状況である。

5位の“複数の攻撃を組み合わせた新しいタイプの攻撃”とは、前項で紹介した “APT”のことであり、既にある複数の手法を織り交ぜて行う攻撃が特徴である。

(6)「2010年情報セキュリティインシデントに関する調査報告書」(NPO 日本ネットワークセキュリティ協会偏)によるとインシデントの特徴は以下のとおりであるとのこと。

・漏洩件数は過去最高であるが、漏洩人数は減少。(1件当たりの漏洩人数の減少)
・漏洩人数では、金融機関は10位であるが、漏洩件数では情報通信業についで多く全体の25%を占めている。
・原因では「管理ミス」が最多。(金融・保険業では発生原因の9割が「管理ミス」)
・漏洩人数では「不正アクセス」が最多
・「内部犯行」は原因全体の4位
・“紙”を媒体にしたものが最多

4. 最近の事故事例の紹介と分析

(1)内部犯行

事例1:センター運用の責任者の不正により、銀行のコンピュータセンターからクレジットカードの顧客データを不正に持ち出し、カードを偽造して現金を引き出した。

事例2:証券会社のシステム幹部が148万件の顧客情報を持ち出し、5万件を名簿会社に売却した。このシステム幹部は、顧客情報を社内のハードディスクにコピーした上で、特殊作業として部下にデータの CD への書き出しを命じていた。

対策としては、権限の分散、プログラム仕様の変更についての承認手続きのあり方などが考えられる。

(2)外部委託による犯行

事例1:外部委託先の社員が顧客データを USB メモリーで自宅に持ち帰り作業を行っていたが、Winny への暴露ウィルスにより顧客の個人情報が流出した。

事例2:外部委託先のプログラマーが顧客のクレジットカード情報を外部記憶媒体を使用して持ち出し第三者に転売した。

事例3:クレジットカード会社のテスト環境から個人情報が大量に流出した。

なお、外部委託先について発生した事例についての再発防止策として以下の対策が考えられる。

・単独で不正が行えないよう、職務の分離および相互牽制を機能させる。
・利用者の職務や職責に応じたアクセス権限を設定、必要最小限の人員に制限する。
・外部委託先の安全管理体制を確認する。(自社と同レベルであるか確認する)
・情報を取り扱う場所をあらかじめ決めておき、その遵守状況を確認する。また PC および外部記憶媒体等について管理を明確にし、入退出管理等の対策と組み合わせて実施する。

※持ち出し制限については、1度ルールを曲げてしまうとどんどん形骸化する。

5. 報告者所感

金融機関は、全ての情報を重要なものと認識しており、セキュリティポリシーは無くてはならないものであると考えていることが良くわかりました。また、顧客が金融機関に求めるものは、個社が考えるもの(=コストに見合ったもの)より、より高いものを求めていることも認識できました。

合わせて最近の脅威の傾向などについても判りやすく良い講演でした。

以上

研究会、セミナー開催報告、支部報告

■ 【第 167 回月例研究会講演録】

会員 No.355　岩崎　昭一（理事）

日時　平成２３年１０月２８日（金）　１８：３０～２０：３０

場所　総評会館

議題　BCMS 適合性評価制度の現況と ISO 化の進展

講師　一般財団法人日本情報経済社会推進協会　情報マネジメント推進センター
　　副センター長　高取　敏夫　氏

＜講演骨子＞

東日本大震災などの影響により、最近特に、各組織における事業継続についての関心が高まっており、BCP（事業継続計画）策定にとどまらず、BCMS を構築・運用する動きが活発化している。このような状況を踏まえ、2010 年 3 月に正式運用が開始された BCMS 適合性評価制度の現況や ISO 化の状況など について概説する。（月例会案内に掲載）

＜講演概要＞

最初に、事業継続に関する現況について、内閣府の「特定分野（電気、通信、ガス等詳細は後述）における事業継続に関する実態調査」を引用して説明があり、その後 BCMS 及び BCMS 適合性評価制度に関する説明があった。主な項目は次のとおりである。

（１） BCMS の概要
　　BCP／BCM の定義、BCMS の定義、BCMS のライフサイクル、BCMS の適用範囲、BCMS の要求事項　等

（２） BCMS 適合性評価制度の概要
　　制度の背景、BS 25999-1:2006、 BS 25999-2:2007、目的、事業分野、認証機関、認証取得組織、BCMS 保証、認証範囲　等

（３） BCMS の ISO 化の現況
　　ISO／TC223、国際規格策定の時期
　　ISO/IEC27031：2011、BS 25999-2 と ISO/CD 22301 との対応表等

＜講演のポイント＞

事業継続マネジメントシステムの有効活用

・企業・組織において緊急事態への事前の対策として、事業継続計画（BCP）の策定に止まらず、BCMS を構築・運用する動きが活発化している。

・災害リスクへの対応については、BCMS を有効に活用することで、BCP の実効性を高めるとともに、組織のレジリエンシーを向上させることができる。

（注）レジリエンシー（Resilience, -cy）：はね返り、弾力（辞書的意味）（筆者追記）
　レジリエンシーとは、企業や組織が事業を停止してしまうような事態に直面したときにも、受ける影響の

範囲を小さく抑え、通常と同じレベルで製品・サービスを提供し続けられるような能力をいう。
BS 25999-1 では、「インシデントに影響されることに抵抗する組織の能力」と定義されている。

＜講演内容＞

１．事業継続に関する実態調査

（１）内閣府中央防災会議では、今後１０年間で BCP 策定の割合を大企業でほぼすべて、中堅企業において過半数を目指す目標である。平成２２年１０月のアンケート調査において、指定公共機関（災害対策基本法第２条５項）では、策定済みが３６％（平成２０年度）から５８％（平成２２年度）に増加している。また策定中までの合計は、７０％から８０％に増加している。

（２）地域別では、東海地震、首都直下地震に対する BCP の策定が進んでいる。

（３）平成２２年の調査は東日本大震災前のものであり３月１１日発生した地震、津波は反映されていない。

（４）BCP を策定する組織は、徐々に多くなってきているが、今後、BCP の実効性を高め本当に役立つものにしていくことが重要であり、今後の推移を見守りたい。

（注）「特定分野における事業継続に関する実態調査」については、内閣府防災会議（防災担当）ホームページを参照されたい。（筆者追記）
URL：http://www.bousai.go.jp/kigyoubousai/topics/index.html

２．BCMS の概要

（１）BCP（Business Continuity Plan）

組織が予め定めた許容可能なレベルで、その重要な活動を実施し続けることを可能とするため、何らかのインシデント発生時に備え、開発され、まとめられ、維持されている文書化された一連の手順及び情報の集合体。

（２）BCM（Business Continuity Management）

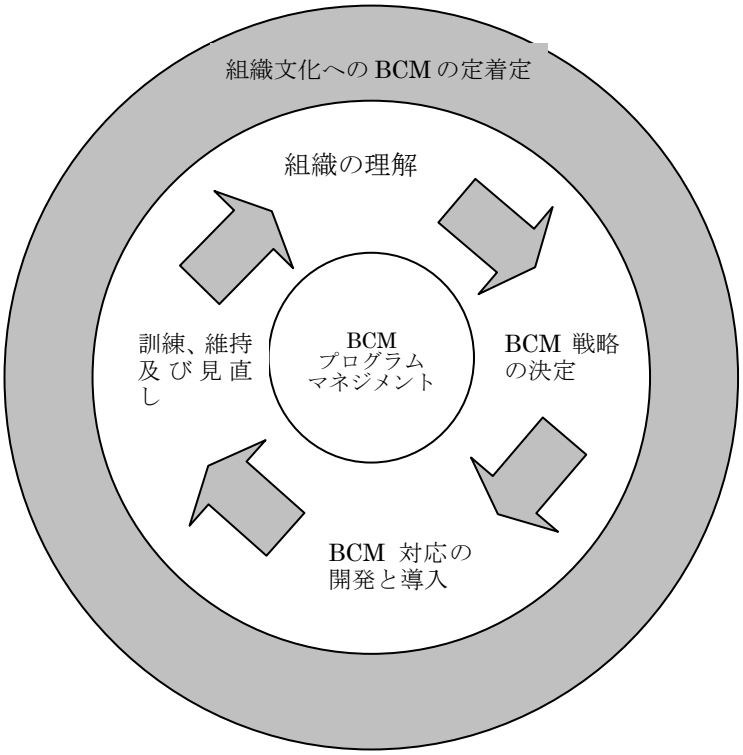
組織への潜在的脅威や、そうした脅威が現実となった場合に引き起こされる可能性のある事業運営上の影響を特定する包括的なマネジメントプロセス。このプロセスにより、組織の主要なステークホルダー（利害関係）の利益や、組織の評判、ブランド、および価値創造活動を守ることについて効果的に対処できるようになり、組織のレジリエンシーを構築するためのフレームワークが提供される。

（３）BCMS（Business Continuity Management System）

BCP／BCM を策定し、BCM ライフサイクル（事業継続の確立、導入、運用、監視、レビュー、維持及び改善）が効果的に運用管理され、改善されることを確実にするマネジメントシステム（「事業継続マネジメントシステム」）をいう。

（４） BCM ライフサイクル

BCM ライフサイクル



BCM プログラムの適用範囲と構造は多様であり、どれだけの労力を掛けるかは個々の組織のニーズによって変わるが、本質的な要素は実行する必要がある。

・BCM プログラムマネジメント
・組織の理解
・事業継続戦略の決定
・BCM 対応の開発と導入
・BCM の訓練、維持管理及びレビュー
・組織文化への BCM の導入

公共・民間・非営利・教育・製造などあらゆる分野のあらゆる規模で実装できる。

（出典：BS 25999-1:2006）

・BCM プログラムマネジメント

BCM プロセスの中核である。効果的なプログラムマネジメントにより、事業継続に対する組織のアプローチが確立される。

・組織の理解

BCM ライフサイクルの要素の狙いは、組織の主要な製品及びサービス、並びにそれをサポートする重要な活動及びリソースの洗い出しを通じて、組織の理解を可能とする。これらの要素は、BCM プログラムを組織の目標、義務、法令で課せられた義務と確実に一致させるべきである。

・事業継続戦略の決定

BCM ライフサイクルの要素は、「組織の理解」に続くものである。事業インパクト分析（BIA）の結果、組織は自らの目標達成を可能にするための適切な継続戦略を選択できる状態にある。

・BCM を実現する手法の開発と実装

BCM ライフサイクルの要素は、重要な活動の継続、並びにインシデントマネジメントを確実なものとするための適切な計画及び取決めを開発し実装することに関するものである。

・BCM への取組みに関する訓練、維持管理、レビュー

BCM ライフサイクルの要素は、訓練及びレビューによって、組織における BCM の有効性が確認され、

最新の状態に維持するよう徹底するものである。

・組織文化への BCM 導入

事業継続を成功させるためには、事業継続は組織の規模や業種にかかわらず、組織のマネジメント手法の一部とならなければならない。BCM プロセスの各フェーズにおいて、組織に BCM 文化を導入し、強化する機会を捉まえる。（以上出典：BS 25999-1:2006）

以上説明したように、現在、BCP／BCM まで進んでいる企業は見受けられるが、BCMS まで進んでいるところは少ない。重要なことは、BCM サイクルをマネジメントシステムとして実際にサイクルを回して BCP の実効性を高めていくことである。

３．BCMS 適合性評価制度

BCMS 適合性評価制度について、詳細な資料を入手したい方は、JIPDEC のホームページを参照されたい。（筆者追記）

（１）BCMS 適合性評価制度の背景

・自然災害、人的災害、取引先の破綻、システム障害等の脅威が発生した場合、事業継続を図る上で影響を及ぼす様々なリスクに対して、どの様に対応を図っていくかは、組織にとって大きな課題である。

・このような不測の事態においても、事業そのものを中断（混乱）することなく、継続・維持するための方針や手続きをまとめたものが BCP である。BCP の作成を含め、事業継続の戦略的な運営管理の手法が BCM である。

・そして、BCM ライフサイクルが効果的に運用管理され、改善されることを確実にするマネジメントシステムが BCMS である。

・BCMS は組織の事業継続を脅かす潜在的な脅威や、それらの脅威が現実となった場合に引き起こされる事態への対応を効率的、効果的に行うための包括的なマネジメントプロセスであり、組織のレジリエンシーを高めるための仕組みである。

（２）BCMS 適合性評価制度とは

BCMS は、組織にとっての重要な業務・サービスが停止したときの影響を最小限に抑え、いかに事業を継続するかという視点で、組織の現状を理解し、事業継続計画を策定し、演習により計画の実行性評価を行いシステム運用するものである。BCMS 適合性評価制度は、2010 年３月に正式に発足し、評価は、BS 25999 に基づき実施している。

（３）BCMS 適合性評価制度の目的

・BCMS 適合性評価制度は、社会の期待に応えられるように、世の中の役に立つ、信頼性のある制度とする。

・BCMS 適合性評価制度は、組織における事業継続の能力を向上させることにより、わが国産業の健全な発展に貢献することを目的とする。

・BCMS 適合性評価制度は、ＢCMS の普及・啓発活動を通じて、産業界における事業継続の取り組みを拡大する。

（4）BCMS の事業分野

事業分野は、一般事業分野と特定事業分野からなる。

・一般事業分野は、特定事業分野を除いた全事業分野とする。

・特定事業分野は、BCMS の対象事業が重大な社会的影響を及ぼす事業分野であり、かつ BCMS の対象事業が高度で特殊な専門性を必要とする事業分野をいう。（表１参照）

表１　BCMS の特定事業分野の分類

No.	特定事業分野の区分	特定事業分野の説明
1	救急医療	三次救命救急医療に関わる分野 例：救命救急センター
2	核燃料	核燃料施設関連分野のうち、核燃料の開発、製造、運用、保管、廃棄を扱う分野 例：ウラン濃縮事業
3	電気、ガス、水道の供給	電力、ガス、水道の供給に関わる分野 例：電力会社
4	旅客事業	鉄道、海運、航空の交通機関のうち、旅客の運輸を対象にする分野 例：航空会社

（5）BCMS 認証機関

６認証機関（１機関は、審査中）（平成２３年９月現在）

（6）BCMS 認証取得組織

２６組織（平成２３年１０月末現在）

認証取得組織は、多岐にわたっているが IT 企業が多く含まれている。

（7）BCMS 認証の価値・意義

・BCMS 認証は、組織が構築した BCMS が規制、顧客及び事業上の要求事項、製品及びサービス、採用しているプロセス、並びにその利害関係者の要求事項を満たしていることを保証することである。

・組織は大規模なインシデント、若しくは事業中断などに直面したとき、事業の復旧及び事業継続を確実にすることを期待できる。

・BCMS を開発、導入及び運用し、教育・訓練、演習、維持及びレビューを通じて重要業務を RTO（目標復旧時間）内に復旧させることを確実にすることが期待できる。

（8）BCMS 認証の保証

・組織の BCMS が、規格要求事項に適合し、明示した方針及び目標を一貫して達成でき、有効に実施されていることを、その顧客及び利害関係者に価値を提供するものである。

・BCMS 認証では、特定した脅威が現実になった時に、組織の重要業務が継続され、事業継続性を向上

させる仕組みが確立・維持されている可能性の高いことを保証するものである。
・想定する脅威に対して、組織の重要業務が中断（混乱）しないことを保証するものではない。

（9）認証基準規格等
・対訳版　BS 25999－1　事業継続マネジメント－第 1 部：実施規範
・対訳版　BS 25999－2　事業継続マネジメント－第 2 部：仕様
・対訳版　ISO PAS 22399 社会セキュリティー緊急事態準備と業務継続マネジメント　ガイドライン
・BCMS ユーザーズガイド BS 25999－2：2007 対応－（JIPDEC 発行）

4．BCMS の ISO 化の現況

BCMS の ISO 化については、ISO／TC223（社会セキュリティ）において検討がすすめられており、2012 年に国際規格 ISO/IEC 22301 として制定される予定である。（未公開資料）

なお、現行の認証基準である BS 25999-2 と ISO/CD 22301 との対応については、大きな差異はなく、ISO への移行は可能である。（対応表は省略）

5．その他（Q&A）

Q１：BCMS の特定事業分野の分類において、通信・放送分野が含まれていない。東日本大震災の教訓から当然含まれるものと考えられるがなぜか。

A1：本制度の発足は、東日本大震災以前のものであり、検討段階で話題にはなっていたが、最終的に含まれていない。今後の検討課題になると思われる。

以上

注目情報（11/1～11/30）

● トピック

1. IPA「定量的プロジェクト管理ツールの分析レポーティング機能」公開

ソフトウェアの品質の確保や納期の遵守のためには、検出不具合数や工数の進捗具合など、プロジェクト進行過程で測定する定量的なデータを用いて品質や進捗の状況を適切に把握することで、リスクを可視化し問題を早期に発見する「定量的プロジェクト管理」が求められます。

IPA（独立行政法人情報処理推進機構、理事長：藤江　一正）は、「定量的プロジェクト管理ツール」を 2012 年 3 月末頃公開する予定ですが、今回「分析レポーティング機能」を先行して公開することになりましたのでお知らせします。 ダウンロードしてご利用ください。　URL：　http://sec.ipa.go.jp/reports/20111114_2.html

2. IPA「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド改訂 2 版」公開

～新たな設計対策を盛り込んだ改訂第 2 版の公開～2011 年 11 月 30 日

IPA（独立行政法人情報処理推進機構、理事長：藤江　一正）は、主催する「脅威と対策研究会」において「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」の改訂第 2 版をまとめ、2011 年 11 月 30 日（水）から IPA のウェブサイトで公開しました。　URL：　http://www.ipa.go.jp/security/vuln/newattack.html

3. JAIPA「沖縄 ICT フォーラム 2011 サイバーセキュリティと通信の秘密　～Security Day in Okinawa～」

社団法人日本インターネットプロバイダー協会（JAIPA）では、次の日程で、ご参加ご希望の方は、ご案内ページ下部の「申し込み方法」をご確認ください。

沖縄 ICT フォーラム 2011　サイバーセキュリティと通信の秘密　～Security Day in Okinawa～
日時　2011 年 12 月 15 日（木）～16 日（金）
場所　場所：沖縄大学　http://www.okinawa-u.ac.jp/shisetsuAccess.php
主催　社団法人日本インターネットプロバイダー協会（JAIPA）
※その他概要、申し込み等は次の URL を確認ください。　http://www.jaipa.or.jp/topics/?p=459

4. 財団法人日本規格協会「JIS Q15001:2006」解説（2011 年改訂）」公表

財団法人日本規格協会より、同協会発行の JIS Q15001:2006（個人情報保護マネジメントシステム-要求事項）について、解説を 2011 年改訂したとの公表がありました。

http://www.webstore.jsa.or.jp/webstore/JIS/html/jp/expl/jis_q_15001_000_000_2006_expl_j_ed10_ch.pdf

全国のイベント・セミナー情報

■ 【東京・月例研究会】

【12 月の月例研究会】

1. テーマ　「量子コンピュータの概要と研究・開発の状況」
2. 日時　2011 年 12 月 21 日（水）　18 時 30 分～20 時 30 分
3. 場所　御茶ノ水　総評会館
   千代田区 神田駿河台　3-2-11　電話：03-3253-1771（代）
   （地下鉄千代田線　新御茶ノ水　Ｂ３直結、または　ＪＲ御茶ノ水駅　聖橋出口 5 分）
4. 講師　ＮＴＴ先端技術総合研究所
   物性科学基礎研究所　量子光物性研究部長　都倉　康弘　氏
5. 会費　SAAJ 会員 2,000 円　非会員 3,000 円

■ 【システム監査実務セミナー４日間コース】（再掲）

日本システム監査人協会では、設立目的のひとつである「システム監査人の実務能力の維持・向上」のため、毎年数回、セミナーを開催しています。

今回ご案内するセミナーは、COSO-ERM モデルが提唱する、企業のリスク低減を図るためのシステム監査を目指す、「システム監査実務セミナー」（４日間コース　１泊２日２回）です。

企業の経営戦略及び業務の有効性と効率性の向上を図るためには、情報システムの活用が必須であり、その評価・改善を進めるためには、システム監査を実施することが有効です。

これまで実施されてきた業務監査（システム監査）では、現場の業務評価の視点を重視した監査が多く見受けられています。

今後は、コーポレートガバナンス、内部統制の面から、業務評価の視点に加えて、経営リスクに対する業務システムの有効性、効率性、安全性の向上の観点からの評価・改善提案が重要になってきます。

本セミナーは、当協会のシステム監査事例研究会で実施した、「システム監査サービス」の実際の監査事例を教材として、ロールプレイを中心とした演習ベースのきわめて実践的なコースで、全社的リスクマネジメントの枠組み（①経営戦略への貢献、②業務の有効性と効率性、③報告の信頼性、④関連法規の遵守）に ついてよりよく理解し、経営に役立つシステムの実現に資するシステム監査の方策を理解・修得することを目標にしております。

なお、本セミナーを受講した後、事後課題を提出頂き、その内容が適切であると判断された場合には、当協会が認定する公認システム監査人の認定に必要なシステム監査実務を 1 年間経験したものとみなされます。

本セミナーは、IT コーディネータ協会の「専門知識研修コース」(5.5 ポイント相当)に認定されています。

1. 日程及び会場
   平成 24 年 1 月 21 日(土)～22 日(日)
   平成 24 年 2 月 4 日(土)～5 日(日)　　＜1 泊２日２回＞
   どちらか一方のみの参加は不可

※　原則として、宿泊必須となりますが、事情により宿泊が難しい場合は、ご相談ください。

時間：土曜は 10:00～21:00、日曜は 09:00～15:00

（進行状況により若干の変更が生じる場合があります。）

会場：　晴海グランドホテル

〒104-0053 東京都中央区晴海 3-8-1

電話番号： 03-3533-7111

（最寄り駅　都営地下鉄大江戸線勝どき駅下車徒歩８分）

2. 費用　168,000 円（日本システム監査人協会会員）

189,000 円（一般）

（費用には、主教材費・宿泊費・食事代・消費税が含まれます。）

3. 副教材

情報システム監査実践マニュアル(第 2 版)　森北出版社　5,460 円

お近くの書店等にてご購入ください。

※工業調査会版の同名書をお持ちの場合は、内容は変わりませんので、新たに購入する必要はありません。

4. 受講していただきたい方

情報処理技術者(システム監査)資格保有者もしくは同等の知識を有する方、または内部監査、システム監査の経験がある方

（上記条件に当てはまらない方は、お問合せください）

1)　企業・官公庁にお勤めの方

：監査部門（内部監査部・室、内部統制部・室、監査役室など）の方

：業務改善部門（企画部・室、事務管理部・室、など）の方

：経営戦略・予実算管理部門（企画部・室、総務部、経理部など）の方

2)　教育・研究者の方

：経営学の部門で教育・研究に携わっている方

：情報学の部門で教育・研究に携わっている方

3)　個人の方

：システム監査の実際を体験してみたい方

：システム監査技術者試験には合格したもののシステム監査参加機会のない方

：公認システム監査人の資格認定を目指している方

：CISA を取得したもののシステム監査参加機会のない方

：監査業務への異動、転職を目指されている方

6. 募集人員　定員 20 名（最少催行人員 10 名）

7. 受講申し込み方法

以下の URL からお申し込みください。

http://www.saaj.or.jp/kenkyu/jitsumuseminar19.html

会報編集部からのお知らせ

１．会報投稿記事 2010 / 2011 アワード開催
２．会報記事への直接投稿（コメント）の方法
３．投稿記事募集

□■ １．会報投稿記事 2010 / 2011 アワード開催

会報を電子化を機会に、ショートエッセイ、「めだか」を連載始めました。
また、投稿された原稿には、それぞれの工夫が施されたものも多く、できるだけ原稿のイメージをお伝えするため電子ファイルで投稿された原稿をそのまま採用させていただくよう、標準フォームを設定しました。
これにより、誤字脱字のチェックなど最小の編集で、記事を発行するようにして、従来の隔月サイクルから月次発行サイクルに変更してお届けするようにしました。
会報の全体記事は、20－40ページにもなるため、個別の記事ごとにも閲覧できるようにしました。

さらに、会報記事の投稿者に図書カードを配布しておりましたが、次のように年間アワードの方式に変更します。
これにより、投稿記事や投稿者個人の学習、知識、経験を広く認知していただくことができます。

つきましては、次の通り、会員の投票形式により、受賞記事を選んでいただく方式を採用します。
年間アワードの実施に伴い、従来の図書カード配布方式は、なくなります。

■対象投稿記事
1）2010 年会報アワード　:2010/1-12 までの会報に掲載された記事を選定の対象とします（初回のみ）
2）2011 年会報アワード　:2011/1-12 までの会報に掲載された記事を選定の対象とします（毎年）
3）アワードの種類:
SAAJ めだか賞
論文賞、
奨励賞　など、3点を選定し、記念品を贈呈する予定。

■選定方法　:
投票期間の開始までに、対象記事タイトルを一覧できる投票用の URL を案内します。
投票には、SAAJ の会員が1票を投票できます。会員は、候補記事の中から、受賞にふさわしいと思う記事を選んで、期日内に投票いただきます。期間内に投票された投票を単純集計し、得票数の多い記事をアワードの対象とします。

■投票期間:
12/16 より 12/31　の 23:59 まで（当月の記事を配信、読んで頂いた後で投票してください）

会報記事への直接投稿（コメント）の方法、おしらせ

□■ ２．　会報の記事に直接コメントを投稿できます

会報の記事は、
1）PDF ファイルの全体を、URL（ http://www.skansanin.com/saaj/ ）へアクセスして、画面で見る
2）PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る
3）会報 URL（ http://www.skansanin.com/saaj/ ）の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。
もっと突っ込んだ、便利な利用法はご存知でしょうか。

気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。
コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。
動画でも紹介しますので、参考にしてください。
（ http://www.skansanin.com/saaj/ の記事、「コメントを投稿される方へ」 ）

□■ ３．ＳＡＡＪ会報編集担当より　お知らせ

会員の皆様からの、投稿を募集しております。分類は次の通りです。

１．めだか　　（Word の投稿用テンプレートを利用してください。会報サイトからダウンロードできます）
２．会員投稿　（Word の投稿用テンプレートを利用してください）
３．会報投稿論文　（論文投稿規程があります）

これらは、いつでも募集しております。 気楽に投稿ください。
特に新しく会員となられた方（個人、法人）は、システム監査への想いやこれまで活動されてきた内容で、
システム監査にとどまらず、IT 化社会の健全な発展を応援できるような内容であれば歓迎いたします。

次の投稿用アドレスに、テキスト文章を直接送信、または Word ファイルで添付していただくだけです。
投稿用アドレス：saaj-kaihoh ☆ yahoogroups.jp （☆は投稿時には＠に変換してください）

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

【本部・理事会議事録】(会員サイトから閲覧ください。パスワードが必要です)

■編集後記に代えて、雑感

現在、会報発行は編集委員の持ち回りで記事集め、編集を行っています。前回は藤野さん、今回は、仲さんのご担当でした。電子化してこれまで、編集後記を記載していませんでしたが、個性の違いが見えますでしょうか。

さて「会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します」といいながら、まだか、いつ開催するのか、という問い合わせを受けます。保守的な監査人にも、新しい技術への関心は不可欠ですね。

まだ日程は決めておりませんが、まずは、年間アワードの仕組みをスタートさせてから開催しようと予定しています。

そのときモデルとする仕組みが、次の「電子化を背景にしたビジネス形態」の事例です。

動画と画像を組み合わせた情報発信の仕組み、情報提供モデルです。印象はどう変わりますか。

埼玉の文化　　http://saitamabunka.com/

埼玉新都心の情報発信　http://shintoshin.biz/

これらのスタイルは今年の早い時期に紹介を予定していました。現在スマホ版を準備中です。これらの仕組みに興味のある方、舞台裏を解説する予定です。運用にはツール等のライセンス費用が必要です。

新しい商品、サービスや技術が紹介されるので、スピードって大切だなと実感します。(竹下)

＝＝

■発行：　NPO 法人　日本システム監査人協会　会報編集部

〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F

■ご質問は、下記のお問い合わせフォームよりお願いします。

【お問い合わせ】　http://www.saaj.or.jp/toiawase/

■送付停止は、購読申請・解除フォームに申し込んでください。

【送付停止】　http://www.skansanin.com/saaj/

Copyright(C)2011、NPO 法人 日本システム監査人協会

掲載記事の転載は自由ですが、内容は改変せず、出典を明記していただくようお願いします。

■□■ＳＡＡＪ会報担当

編集：　竹下和孝、仲　厚吉、安部晃生、成 楽秀、桜井由美子、清水恵子、山田 隆、片岡 学、

木村陽一、藤野明夫　　投稿用アドレス：saaj-kaihoh☆yahoogroups.jp（☆は安全対策）